SAP Community

Ask a Question Write a Blog Post Login

Alessandro Banzer

April 28, 2014 | 2 minute read

Rule set – Rules & Rule Types

19 26 78,089

Follow

Like

RSS Feed

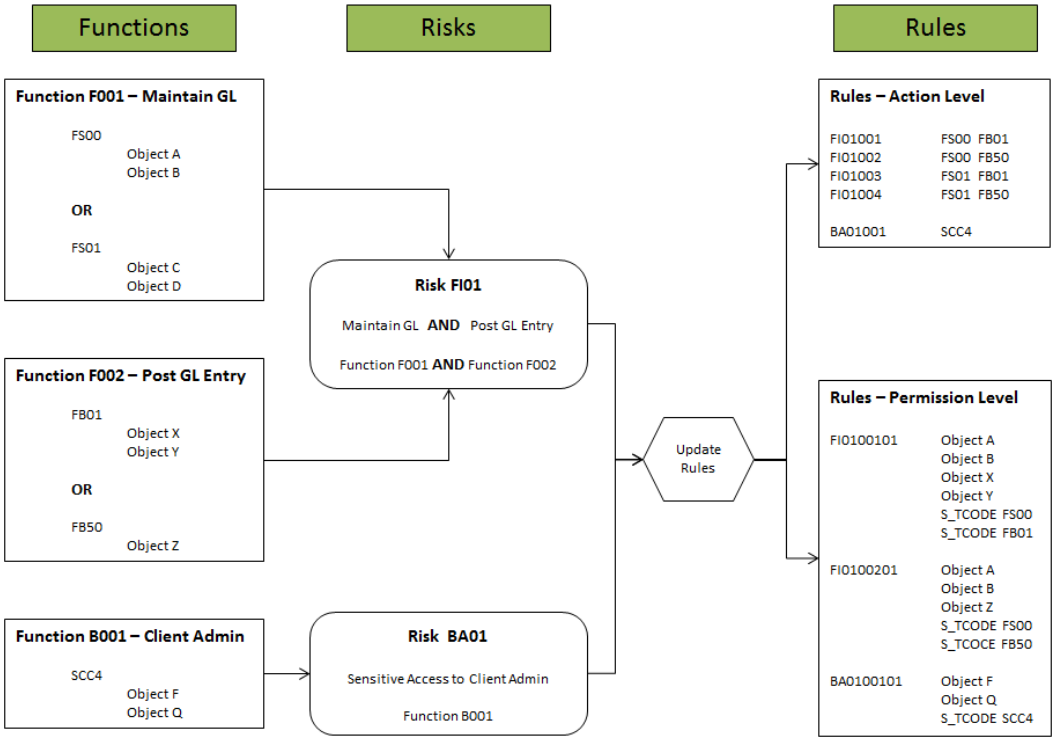
In regard to my document about Rule Set / Business Risks I would like to give some detailed information about rules and rule types. As we learned rules (or risk rules) are possible combinations of transactions and permissions for a business risk.

Rules must be generated when ever risk contents change. This can be done in SPRO (GRC > Access Control > Access Risk Analysis > SOD Rules > Generate SoD Rules). Generally rules are combinations of actions and aren't maintained manually (done automatically by the program).

The number of rules defined from a risk is determined by

- the number of action combinations, and
- permission/field value combinations contained in each function of the risk.

The following graphic shows the rule structure in more detail:



Now let me give you a short overview of the different types of rules considered by GRC.

Transaction Rules

Rule components are as follows:

- System
- Conflicting Actions
- Rule ID
- Risk Level
- Status

Example (from the graphic above):

F001001: Maintain fictitious GL account & hide activitiy via postings

F001001 – Risk ID

F001**001** – Action code combination number (represents Conflicting Actions)

Permission Rules

Rule components are as follows:

- System
- Object
- Field
- Rule ID

- Risk Level
- Status

Example (from the grapic above):

F00100101: Maintain fictitious GL account & hide activity via postings

F00100101 – Risk ID

F001**00**101 – Action code combination number

F00100**101** – Object combination number

Critical Action

List of actions considered critical. Option to run at both Action and/or Permission level. Critical Actions are created same way as Segregation of Duty risks, exept Risk Type = Critical Action, and can contain only 1 function (as shown above with SCC4).

Critical Permission

List of objects/permission considered critical. Created same way as Segregation of Duty Risks, exept Risk Type = Critical Permission, can contain only 1 function, and function cannot contain actions.

Critical Roles and Profiles

Roles and profiles considered critical. Critical roles and profiles will be excluded from analysis if the configuration parameter 1031 (Ignore Critical Roles & Profiles) is set to YES.

Organizational

Used to eliminate false positive SOD reporting based on organizational level restrictions for users. Organziational rules should not be created for mass org level reporting as it should only be enabled for functions that you specifically need to segregate. Most companies are controlling what data a user has access to via role assignment. There are only very few companies who have a business need to create org rules. Please find more detailed information in Organizational Rules in GRC Access Control.

Supplementary

Additional security parameters other than authorizations a user must have to enable access. First checks to see if the user exists in the supplementary table, then checks if conditions are met. Based on exclusion setting, it will include or exclude the user in the risk analysis.

Please share and contribute in this document to make it better.

Looking forward to hear from you.

Best regards,

Alessandro

Alert Moderator

Assigned Tags

SAP Access Control

Governance Risk And Compliance

governance risk and compliance sap grc

grc 10

rule set

rule structure

Similar Blog Posts

SAP Success Factors Employee Central and its integration with SAP GRC Risk Analysis & Access Request

By Ritika Mehrotra May 12, 2020

Helpful transactions, tools, programs, tables, etc. for a SAP GRC Consultant

By Alessandro Banzer Oct 01, 2014

ARA - For the new kid on the block

By S A Aug 27, 2014

Related Questions

GRC AC Role Removal without role owner approvals

By Michael Hughes Jul 10, 2017

Business Role showing Role Level Risk after Rule Set Upload from one GRC system to Another

By Syed Imam May 21, 2023

SAP GRC Access Control Rule Set: Critical Permission Rule Does Not Work

By Reza Ahoui Oct 25, 2019

19 Comments

You must be Logged on to comment or reply to a post.

Mamoon Rashid
April 28, 2014 at 9:48 am

Nice Documnet covering useful information. Could you give one example of Org rule.

Thanks,

Mamoon

Like 0 | Share

Alessandro Banzer | Blog Post Author
April 29, 2014 at 6:43 am

Dear Mamoon,

thanks for your feedback. Let me create a document explaining organization rules in more detail.

Quick-and-dirty I would say you have a role concept with derived roles where the leading organizational level is the company code. Assume that you have a SOD risk between FB60 (posting of vendor invocies) and FK02 (changing vendor master data). A combination of transaction FK02 and FB60 is a SOD conflict. A user who gets both roles assigned would have a combination of both transactions which is conflicting according to your rule set and would shop up as a SOD conflict.

This could be false positive as the user can actually not call FK02 and FB60 for the same company code (assume that FK02 is for company code 1000 and FB60 for company code 2000).

Hope this helps to understand the concept behind organizational rules.

Regards,

Alessandro

Like 0 | Share

Colleen Hebbert

April 29, 2014 at 6:55 am

Hi Alessandro

Your material is great but wondering if some this belongs in the GRC Wiki?

Governance, Risk, and Compliance (GRC) How-To Guides - Business Process Expert - SCN Wiki

There is a document here already SAP GRC Access Control: Organizational Rules and Organizational Level Reporting but is it for an older version

Maybe you could see if you could get access and take on some the pages?

Regards

Colleen

Like 0 | Share

Alessandro Banzer | Blog Post Author

April 29, 2014 at 7:06 am

Hi Colleen,

didn't check if a document is already there yet.

Mamoon Rashid please use the document mentioned by Colleen.

Regards,

Alessandro

Like 0 | Share

Faisal Khan

June 12, 2014 at 4:59 pm

Hi Alessandro,

This is really very helpful. I am enjoying it as you have maintained every detail.

I have a small question. Hope you dont mind me asking this.

Taking your FI01 risk example, I would like to discuss my doubt.

As you said Action rule for FS00 and FB01 is: FI01001, does it mean that it always starts with <Function ID>"001"?

Because I tell you, I have a function F016 (I am on GRC 10, SP#14) and I could see that its "Access Rule ID" starts with "0001"

Please find below screen shot (Rules starting with 0001):

C	D	E	F	G	H	I	J	K	L	M
Access	Access	Access	Access	Busine	Functic	Functic	Action	Access	Permission Object	Field
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ01	0001	S_TCODE	TCD
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ01	0001	C_CSCR_ACT	PS_ACTVT
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ01	0001	C_MLST_BGR	BEGRU
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ01	0001	C_MLST_BGR	PS_ACTVT
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ01	0001	C_MLST_BGR	PS_ACTVT

Please find below screen shot (Rules starting with 0002):

C	D	E	F	G	H	I	J	K	L	M
Access	Access	Access	Access	Busine	Functic	Functic	Action	Access	Permission Object	Field
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ02	0002	S_TCODE	TCD
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ02	0002	C_CSCR_ACT	PS_ACTVT
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ02	0002	C_MLST_BGR	BEGRU
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ02	0002	C_MLST_BGR	PS_ACTVT
F016	Use fictiti	Segregati	High	Finance	PS01	PS01 - Ma	CJ02	0002	C_MLST_BGR	PS_ACTVT

I am quite confused with "0001" interpretation. Going by your example, can I write like:

F016<Function ID>000<Action Rule>01<Permission Rule> (F01600001)?

Is it like in GRC 10, Rules are starting with "000" instead of "001"?

Please help me understand.

Regards,

Faisal

Like 0 | Share

Kevin Tucholke SAP

June 12, 2014 at 7:50 pm

Faisal:

Previously in AC 5.3, when the rules were generated, the numbering convention looks like what is stated above. Risk IDs in 5.3 were limited to 4 chars, then when the rules were generated it would add a 3 char action combination and a 2 char permission ID. So in the example above, the full Risk ID would have been F00100101.

In AC 10.x, the numbering convention has changed. This is now spilt between 2 fields which are Risk ID and Rule ID. Risk ID is exactly what you would think that it is, Rule ID would be the Action Combination. Risk ID in AC10.x can be up to 8 chars now, and the Risk ID is always 4 chars. In AC10.0, the same entry in the example would be Risk ID F001, and Rule ID 0001.

Hope this helps.

Kevin

Like 0 | Share

Faisal Khan
June 13, 2014 at 11:04 am

Hi Kevin,

Thanks for this.

It is clear now.

All the risks would be starting with 0001 access rule id.

There is one note#1310365. This says that in AC 10. the maximum number of rules that can be generated are 1679616 (36*36*36*36)

Regards,

Faisal

Like 0 | Share

Former Member
July 8, 2015 at 4:21 am

Hi Alessandro --- you may want to add here a link to your document on Organizational Rules 🙂 .... Thanks for this.

Like 0 | Share

Alessandro Banzer | Blog Post Author
July 8, 2015 at 7:20 am

thanks for your feedback. I have linked the document 🙂

Like 0 | Share

Faisal Khan
June 15, 2014 at 4:08 pm

Alessandro,

One more question I have (I have already raised a thread for the same):

ARQ: Are "Valid From" and "Valid To" dates are considered for risk analysis???

As you mentioned "Rules Components" for transaction and permission rules, I have not found "Validity" dates as a "component" of the risk analysis

May you confirm if ARA considers validity period also?

Because, in ARQ when a request is raised for 2 conflicting roles assignment with different future assignment dates (no overlapping), still violations are shown!

May you please advise?

Regards,

Faisal

Like 0 | Share

Former Member
November 26, 2015 at 6:28 am

Its really a very nice document related to rule set, rule types in structured manner. Thanks to Alessandro.

Regards,

Deepak Singh

Like 0 | Share

Former Member
March 16, 2016 at 3:35 pm

Dear Alessandro,

Thanks for very informative and precise document.

can you please guide me on the below points.

what is the maximum no of function ids that can assign to a risk id?

what is the best practice or thumb rule to create function ids and risk ids

Regards

Mohammed

Like 0 | Share

Alessandro Banzer | Blog Post Author
March 17, 2016 at 7:13 am

Mohammad,

I have never tried the limit of functions within a risk. And to be honest I don't see a case where you need more than two (or three) functions. Segregation of duties usually consists two functions, sometimes it's required to have three within the same risk. Best if you try and once you hit the max open an OSS and ask SAP for a solution.

Best practise for function / risk creation depends on your requirements. I personally keep an eye on SU24 values that must be maintained accordingly to get the proper default values when creating a function. Apart from that it depends how you create your functions. It can be either done in GRC directly or via Excel upload. In case I use the Excel upload, I export SU24 values from the backend and prepare in Excel accordingly.

Hope this helps.

Regards,

Alessandro

Like 0 | Share

Bruce van Rooyen
June 24, 2016 at 10:38 am

Thanks for the detailed document Alessandro. I have a question that I am battling to get more information on.

Where and when is updates to the Rule set supplied by SAP and when was the last update on the Rule set.

We have migrated to HANA/EHP7 which delivered some new transactions (ending with "H") which is not in the Rule set and we are looking at implementing simple Finance which also brings new transactions and other transactions are obsolete. Is there an update to the rule set available that will include these new transactions?

Regards

Bruce

Like 1 | Share

Former Member
February 8, 2017 at 2:29 pm

Thanks for the detailed document Alessandro.

I have a questions around creating a SOD risk with 3 functions.

How would my Rules be like?

I think it would be Action1(Function1) v/s Action2(Function2) v/s Action3(function3). Can you confirm based on your expertise?

Thanks in advance.

Like 0 | Share

Former Member
July 30, 2017 at 12:11 pm

Thx for the super documentation BR Hp

Like 1 | Share

Michael Oliver Lim
July 3, 2019 at 2:42 pm

Hello Alessandro,

May I ask if how do you compute the number of rules per risk?

I am experiencing the Rules Generation error in GRC 5.3 The error is " *"Error while executing the Job:ERROR: Risk: M118 has exceeded the maximum number of rules (46,655) that can be generated for a risk"*

Base from SAP Note 1310365 , the formula is Distinct Rules = no. of functions per risk x no. of actions per function

for example risk M118 has 2 functions , F000010 and F00A100

F000010 - 36 actions

F00A100 - 337 actions

The number of distinct rule for risk M118 is 24, 264 rules (2x 36 x 337)right ?

May I ask the possible reason why the the rules has exceeded 46,655?

Is there other formula to compute the number of distinct rules like checking the function permission file which includes Actions / tcode and Auth objects and Auth field?

Like 0 | Share

Nalla Ravinder

April 6, 2020 at 6:46 am

Hi All

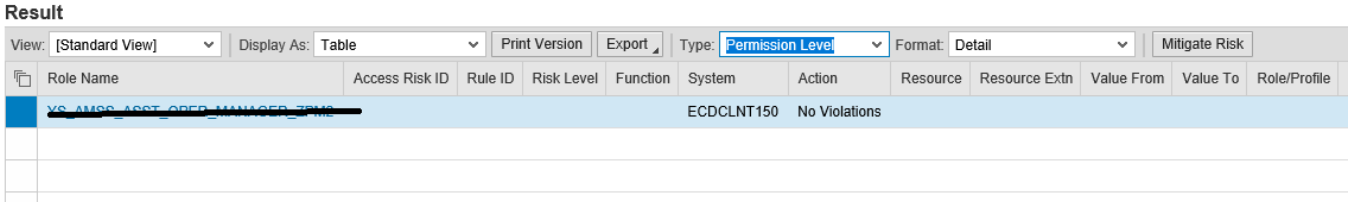
I am getting action level risk with single action and single rule id, (normally each rule id two or more values for a risk) we have one function with Action IW32 and other function with permission level values only.

When I am adding the object values to the role permission level and action level risks are getting fine with Action and PG(Action).

My issue is when I removed the object values at object in the role I am not getting any risks at permission level as expected results. But I am able to see risk at action tab, it should not the case.

Can any one help for this issue. I am missing any jobs or settings. I have generated SOD rules, all sync lobs run successfully.

Ravinder



Result

View: * [Standard View] | Display As: Table | Print Version | Export | Type: Action Level | Format: Detail

Role Name	Access Risk ID	Rule ID	Risk Level	Function	System	Action	Role/Profile
[redacted]	ZPM02	008T	Medium	ZPM11	ECDCLNT150	IW32	[redacted]
[redacted]	ZPM02	0091	Medium	ZPM11	ECDCLNT150	IW37N	[redacted]
[redacted]	ZPM02	0093	Medium	ZPM11	ECDCLNT150	IW38	[redacted]
[redacted]	ZPM02	00BL	Medium	ZPM11	ECDCLNT150	IW32	[redacted]
[redacted]	ZPM02	00BT	Medium	ZPM11	ECDCLNT150	IW37N	[redacted]
[redacted]	ZPM02	00BV	Medium	ZPM11	ECDCLNT150	IW38	[redacted]
[redacted]	ZPM02	00ED	Medium	ZPM11	ECDCLNT150	IW32	[redacted]
[redacted]	ZPM02	00EL	Medium	ZPM11	ECDCLNT150	IW37N	[redacted]
[redacted]	ZPM02	00EN	Medium	ZPM11	ECDCLNT150	IW38	[redacted]
[redacted]	ZPM03	005X	Medium	ZPM11	ECDCLNT150	IW32	[redacted]

Like 0 | Share

Nalla Ravinder
April 16, 2020 at 4:06 am

Hi All

The above issue not able to solve as single action risks are coming due to Permission group. So I have decided and created the Critical Permission Risks for our requirement with change of other values to fix false positive risks in our environment.

And simultaneously We have raised issue with SAP also. They replied back to us same answer for creating the Critical Permission Risk for the our requirements.

Now issue is fixed with as above solution. Thanks for your time and help.

Ravinder Nalla

Like 0 | Share

Find us on

Privacy	Terms of Use
Legal Disclosure	Copyright

Trademark	Cookie Preferences
Newsletter	Support